

In the Specification:

Replace the paragraph beginning on page 6 line 14 with:

Referring now to FIG. 1, a schematic diagram illustrates a server
5 100 used to receive encrypted data from a sending client computer 102
and transmit encrypted data to a receiving client computer 104 through
the Internet 106 using shared private keys. The sending client 102 and
receiving client 104 share their own private key with the server 100, but
do not share their private keys with anyone else.

10

Replace the paragraph beginning on page 8 line 6 with:

FIG. 5 is a block diagram of one embodiment of the non-volatile
memory module 404 located within the clients 102, 104 of FIG. 4. The
non-volatile memory 406 includes an encrypt/decrypt engine 502 for
15 encrypting and decrypting data. The encrypt/decrypt engine 502 can
also be stored in RAM 404. Excellent results can be obtained when the
encrypt/decrypt engine is served up as a Java™ applet to the clients
102, 104. The Java™ applet can be served up with a web page. In
another form, the encrypt/decrypt engine can be sent to the clients 102,
20 104, and then stored on their hard drive.

Replace the paragraph beginning on page 10 line 3 with:

FIG. 8 is a flowchart of a method illustrating how a user having a shared private key passes secure data through a server computer over the Internet. This method is very similar to the process described in FIGS. 6 and 7. The process begins at step 800. A user having a private key shared with the server establishes a session over the Internet with the server by requesting a web page at step 802 using a suitable client. At step 804 the server sends a web page form from the web page forms database 310 to the client. Next at step 806 the user enters data into the web page along with his private key shared with the server. At step 808 the data is encrypted with the encrypt/decrypt engine at the client computer using the user's private key and then the encrypted data is sent to the server. It is explicitly shown at step 808 that the user's private key is the user's personal authentication data. The encryption key is formed from the authentication data. Subsequently, the authentication data is NOT sent to the server and it is NOT used for authentication per se except in so far as both client and server are able to encrypt and decrypt the data using the same key.

20 Replace the paragraph beginning on page 10 line 20 with:

After the processing step is completed at step 814 the server encrypts the processed data using the user's private key that is stored in the user private keys database 304 and sends the encrypted data to the

client. It is not necessary for the client to be the same client that began the process at step 802. The server can be used as an intermediary for passing and processing secure data between clients.

5

E Replace the paragraph beginning on page 11 line 4 with:

10

At step 816, the client receives the secure data and the user enters their private key. At step 818 the encrypted processed data is decrypted with the user's private key, which is now available to the client, using the encrypt/decrypt engine 502. At step 820 the client can access the data or the user can view the data, and at step 822 the process ends.